

# **EXHIBIT 8**

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability												
A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:	<p>Cisco Advanced Malware Protection (AMP) includes <i>a computer program product embodied on a non-transitory computer readable medium</i> (e.g., Cisco security appliances and/or firewalls, etc.), <i>the computer program product comprising</i>:</p> <p>“Deployment Options for Protection Everywhere</p> <p>Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, the AMP solution can be deployed at different control points throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:”</p> <table border="1"> <thead> <tr> <th>Product Name</th><th>Details</th></tr> </thead> <tbody> <tr> <td>...</td><td>...</td></tr> <tr> <td>Cisco AMP for Networks</td><td>Deploy AMP as a network-based solution <u>integrated into Cisco Firepower NGIPS security appliances.</u></td></tr> <tr> <td>Cisco AMP on Firewalls and ASA with FirePOWER Services</td><td>Deploy <u>AMP capabilities integrated into the Cisco NGFW or ASA Adaptive Security Appliance firewall.</u></td></tr> <tr> <td>...</td><td>...</td></tr> <tr> <td>Cisco AMP for Meraki MX</td><td><u>Deploy AMP as part of the Meraki MX Security Appliance</u> for cloud-based simplified security</td></tr> </tbody> </table>	Product Name	Details	...	...	Cisco AMP for Networks	Deploy AMP as a network-based solution <u>integrated into Cisco Firepower NGIPS security appliances.</u>	Cisco AMP on Firewalls and ASA with FirePOWER Services	Deploy <u>AMP capabilities integrated into the Cisco NGFW or ASA Adaptive Security Appliance firewall.</u>	...	...	Cisco AMP for Meraki MX	<u>Deploy AMP as part of the Meraki MX Security Appliance</u> for cloud-based simplified security
Product Name	Details												
...	...												
Cisco AMP for Networks	Deploy AMP as a network-based solution <u>integrated into Cisco Firepower NGIPS security appliances.</u>												
Cisco AMP on Firewalls and ASA with FirePOWER Services	Deploy <u>AMP capabilities integrated into the Cisco NGFW or ASA Adaptive Security Appliance firewall.</u>												
...	...												
Cisco AMP for Meraki MX	<u>Deploy AMP as part of the Meraki MX Security Appliance</u> for cloud-based simplified security												

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability	
		management with advanced threat capabilities.
<p>code for:</p> <p>accessing at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:</p> <p>each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and</p>	<p><a href="https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p> <p>Cisco Advanced Malware Protection (AMP) includes <i>code for: accessing at least one data structure</i> (e.g., AMP's threat intelligence database, etc.) <i>identifying a plurality of mitigation techniques</i> (e.g., static and dynamic malware analysis and/or outbreak control, etc.) <i>that mitigate effects of attacks that take advantage of vulnerabilities</i> (e.g., memory attacks on an application and/or operating system process, etc.), <i>where: each mitigation technique</i> (e.g., the static and dynamic malware analysis and/or outbreak control, etc.) <i>is capable of mitigating an effect of an attack</i> (e.g., a previously unknown zero-day threat and/or infection like polymorphic malware, compromised application, and/or malware call-back communication, etc.) <i>that takes advantage of a corresponding vulnerability</i> (e.g., a memory attack on an application and/or operating system process, etc.), <i>and</i></p> <p>"This is the power of continuous analysis, continuous detection, and retrospective security: the ability to record the activity of every file in the system and, if a supposedly "good" file turns "bad," the ability to detect it and rewind the recorded history to see the origin of the threat and the behavior it exhibited. AMP then provides you with built-in response and remediation capabilities to eliminate the threat. AMP also remembers what it sees, from the threat's signature to the behavior of the file, and <u>logs the data in AMP's threat intelligence database to further strengthen front-line defenses</u> so this file and files like it will not be able to evade initial detection again."</p> <p><b>"Main Features</b> AMP's continuous analysis and retrospective security capabilities are made possible because of these robust features:</p>	

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability
	<p>...</p> <ul style="list-style-type: none"> <li>• <b>Static and dynamic malware analysis:</b> A highly secure sandboxing environment helps you <u>run, analyze, and test malware in order to discover previously unknown zero-day threats</u>. Integration of Threat Grid's sandboxing and static and dynamic malware analysis technology into AMP solutions results in a more comprehensive analysis checked against a larger set of behavioral indicators.</li> </ul> <p>...</p> <ul style="list-style-type: none"> <li>• <b>Outbreak control:</b> <u>Achieve control over suspicious files or outbreaks and remediate an infection without waiting for a content update. Within the outbreak control feature:</u> <ul style="list-style-type: none"> <li>• Simple custom detections can <u>quickly block a specific file across all or selected systems</u></li> <li>• Advanced custom signatures can <u>block families of polymorphic malware</u></li> <li>• Application blocking lists can <u>enforce application policies or contain a compromised application</u> being used as a malware gateway and stop the reinfection cycle</li> <li>• Custom whitelists will help ensure that safe, custom, or mission-critical applications continue to run no matter what</li> <li>• Device flow correlation will <u>stop malware call-back communications at the source</u>, especially for remote endpoints outside the corporate network"</li> </ul> </li> </ul> <p><a href="https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p>
each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;	<p>Cisco Advanced Malware Protection (AMP) includes <i>each mitigation technique</i> (e.g., the static and dynamic malware analysis and/or outbreak control, etc.) <i>has a mitigation type including at least one of a patch, a policy setting, or a configuration option</i> (e.g., an application blocking list that enforces application policies to stop a reinfection cycle, etc.);</p> <p><b>"Main Features</b> AMP's continuous analysis and retrospective security capabilities are made possible because of these robust features:</p>


## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability
	<p>...</p> <ul style="list-style-type: none"> <li>• <b>Static and dynamic malware analysis:</b> A highly secure sandboxing environment helps you <u>run, analyze, and test malware in order to discover previously unknown zero-day threats</u>. Integration of Threat Grid's sandboxing and static and dynamic malware analysis technology into AMP solutions results in a more comprehensive analysis checked against a larger set of behavioral indicators.</li> </ul> <p>...</p> <ul style="list-style-type: none"> <li>• <b>Outbreak control:</b> <u>Achieve control over suspicious files or outbreaks and remediate an infection without waiting for a content update. Within the outbreak control feature:</u> <ul style="list-style-type: none"> <li>• Simple custom detections can quickly block a specific file across all or selected systems</li> <li>• Advanced custom signatures can block families of polymorphic malware</li> <li>• <u>Application blocking lists can enforce application policies</u> or contain a compromised application being used as a malware gateway and <u>stop the reinfection cycle</u></li> <li>• Custom whitelists will help ensure that safe, custom, or mission-critical applications continue to run no matter what</li> <li>• Device flow correlation will stop malware call-back communications at the source, especially for remote endpoints outside the corporate network"</li> </ul> </li> </ul> <p><a href="https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p>
code for:  receiving information in connection with at least one of a plurality of devices; and	<p>Cisco Advanced Malware Protection (AMP) includes <i>code for: receiving information</i> (e.g., data pertaining to systems affected by malware on the Device Trajectory dashboard, etc.) <i>in connection with at least one of a plurality of devices</i> (e.g., a specific endpoint or computer on which threat activity has been received, etc.); <i>and</i></p> <p>"Powerful innovations like file trajectory and <u>device trajectory [] use AMP's big data analytics and continuous analysis capabilities to show you the systems affected by malware</u>, including patient zero and the root causes associated with a potential compromise. These capabilities help you</p>

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability
	<p>quickly understand the scope of the problem by identifying malware gateways and the path that attackers are using to gain a foothold into other systems.”</p>  <p>...</p> <p><u>Device trajectory further aids a quick analysis of threat activity on a computer by tracking file and network activity at the endpoint in chronological order. You gain complete visibility into the events</u></p>

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability						
	<p>that occurred leading up to and following a compromise, including parent processes, connections to remote hosts, and unknown files that may have been downloaded by malware.”</p> <p><a href="https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p>						
identifying an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information;	<p>Cisco Advanced Malware Protection (AMP) includes <i>identifying an attack</i> (e.g., a previously unknown zero-day threat and/or infection like polymorphic malware, compromised application, and/or malware call-back communication, etc.) <i>on the at least one device</i> (e.g., the specific endpoint or computer on which threat activity has been received, etc.) <i>that takes advantage of at least one of the vulnerabilities</i> (e.g., a memory attack on an application and/or operating system process, etc.), <i>based on the information</i> (e.g., the data pertaining to systems affected by malware on the Device Trajectory dashboard, etc.);</p> <p><b>“Features and Benefits of Cisco AMP for Endpoints”</b></p> <table border="1"> <thead> <tr> <th>Feature</th><th>Benefits</th></tr> </thead> <tbody> <tr> <td>...</td><td>...</td></tr> <tr> <td>Dashboards</td><td>Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a</td></tr> </tbody> </table>	Feature	Benefits	...	...	Dashboards	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a
Feature	Benefits						
...	...						
Dashboards	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a						


## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability	
		comprehensive contextual view so that you can make informed security decisions.
	...	...
	Exploit Prevention	<p><u>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes.</u> The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a payload, and zero-day attacks on software vulnerabilities yet to be patched.</p>
	<p><a href="https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p> <p>“Powerful innovations like file trajectory and <u>device trajectory [] use AMP’s big data analytics and continuous analysis capabilities to show you the systems affected by malware,</u> including patient zero and the root causes associated with a potential compromise. These capabilities help you quickly understand the scope of the problem by identifying malware gateways and the path that attackers are using to gain a foothold into other systems.”</p>	

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability
	 <p>...</p> <p>Device trajectory further aids a quick analysis of threat activity on a computer by tracking file and network activity at the endpoint in chronological order. You gain complete visibility into the events that occurred leading up to and following a compromise, including parent processes, connections to remote hosts, and unknown files that may have been downloaded by malware.”</p>

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability
	<a href="https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)
<p>code for:</p> <p>automatically applying at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device, for mitigating an effect of the attack on the at least one device that takes advantage of the at least one vulnerability;</p>	<p>Cisco Advanced Malware Protection (AMP) includes <i>code for: automatically applying at least two of the plurality of mitigation techniques</i> (e.g., the static and dynamic malware analysis and/or outbreak control, etc.) <i>including at least one first mitigation technique of a first mitigation type</i> (e.g., a first of a specific file, a custom signature, application blocking lists, or custom whitelist, etc.) <i>and at least one second mitigation technique of a second mitigation type</i> (e.g., a second of a specific file, a custom signature, application blocking lists, or custom whitelist, etc.) <i>to the at least one device</i> (e.g., the specific endpoint or computer on which threat activity has been received, etc.), <i>for mitigating an effect of the attack</i> (e.g., a previously unknown zero-day threat and/or infection like polymorphic malware, compromised application, and/or malware call-back communication, etc.) <i>on the at least one device</i> (e.g., the specific endpoint or computer on which threat activity has been received, etc.) <i>that takes advantage of the at least one vulnerability</i> (e.g., the memory attack on an application and/or operating system process, etc.);</p> <p>“Cisco AMP for Endpoints Outbreak Control gives you a suite of capabilities to effectively <u>stop the spread of malware and malware-related activities</u>, like call-back communications or dropped file execution, without waiting for updates from your security vendor. This gives you the <u>power to move directly from investigation to control with a few mouse clicks, significantly reducing the time a threat has to spread or do more damage and the time it normally takes to put controls in place.</u>”  <a href="https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p>

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability				
	<p><b>“Main Features</b></p> <p>AMP’s continuous analysis and retrospective security capabilities are made possible because of these robust features:</p> <p>...</p> <ul style="list-style-type: none"> <li>• <b>Static and dynamic malware analysis:</b> A highly secure sandboxing environment helps you <u>run, analyze, and test malware in order to discover previously unknown zero-day threats</u>. Integration of Threat Grid’s sandboxing and static and dynamic malware analysis technology into AMP solutions results in a more comprehensive analysis checked against a larger set of behavioral indicators.</li> </ul> <p>...</p> <ul style="list-style-type: none"> <li>• <b>Outbreak control:</b> <u>Achieve control over suspicious files or outbreaks and remediate an infection</u> without waiting for a content update. Within the outbreak control feature: <ul style="list-style-type: none"> <li>• Simple custom detections can <u>quickly block a specific file across all or selected systems</u></li> <li>• <u>Advanced custom signatures can block families of polymorphic malware</u></li> <li>• <u>Application blocking lists can enforce application policies or contain a compromised application</u> being used as a malware gateway and stop the reinfection cycle</li> <li>• <u>Custom whitelists</u> will help ensure that safe, custom, or mission-critical applications continue to run no matter what</li> <li>• Device flow correlation will <u>stop malware call-back communications at the source</u>, especially for remote endpoints outside the corporate network”</li> </ul> </li> </ul> <p><a href="https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p> <p><b>“Features and Benefits of Cisco AMP for Endpoints”</b></p> <table border="1"> <thead> <tr> <th>Feature</th><th>Benefits</th></tr> </thead> <tbody> <tr> <td>...</td><td>...</td></tr> </tbody> </table>	Feature	Benefits	...	...
Feature	Benefits				
...	...				

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability	
	Dashboards	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a comprehensive contextual view so that you can make informed security decisions.
	...	...
	Exploit Prevention	<u>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes.</u> The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a payload, and zero-day attacks on software vulnerabilities yet to be patched.
	<a href="https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)	

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability										
<p>wherein the computer program product is operable such that the effect of the attack is mitigated by preventing the attack from taking advantage of the at least one vulnerability;</p>	<p>Cisco Advanced Malware Protection (AMP) includes <i>wherein the computer program product is operable such that the effect of the attack</i> (e.g., a previously unknown zero-day threat and/or infection like polymorphic malware, compromised application, and/or malware call-back communication, etc.) <i>is mitigated by preventing the attack from taking advantage</i> (e.g., exploiting, etc.) <i>of the at least one vulnerability</i> (e.g., the memory attack on an application and/or operating system process, etc.);</p> <p><b>“Features and Benefits of Cisco AMP for Endpoints”</b></p> <table border="1"> <thead> <tr> <th data-bbox="695 654 898 695">Feature</th><th data-bbox="898 654 1545 695">Benefits</th></tr> </thead> <tbody> <tr> <td data-bbox="695 695 898 735">...</td><td data-bbox="898 695 1545 735">...</td></tr> <tr> <td data-bbox="695 735 898 1044">Dashboards</td><td data-bbox="898 735 1545 1044">Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a comprehensive contextual view so that you can make informed security decisions.</td></tr> <tr> <td data-bbox="695 1044 898 1084">...</td><td data-bbox="898 1044 1545 1084">...</td></tr> <tr> <td data-bbox="695 1084 898 1396"><u>Exploit Prevention</u></td><td data-bbox="898 1084 1545 1396"><u>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes.</u> The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a</td></tr> </tbody> </table>	Feature	Benefits	...	...	Dashboards	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a comprehensive contextual view so that you can make informed security decisions.	...	...	<u>Exploit Prevention</u>	<u>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes.</u> The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a
Feature	Benefits										
...	...										
Dashboards	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a comprehensive contextual view so that you can make informed security decisions.										
...	...										
<u>Exploit Prevention</u>	<u>Memory attacks can penetrate endpoints, and malware evades security defenses by exploiting vulnerabilities in applications and operating system processes.</u> The Exploit Prevention feature will defend endpoints from all exploit-based, memory injection attacks—including ransomware using in-memory techniques, web-borne attacks that use shellcode to run a										

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability		
	<table border="1" data-bbox="695 302 1545 378"> <tr> <td data-bbox="695 302 898 378"></td><td data-bbox="898 302 1545 378">payload, and zero-day attacks on software vulnerabilities yet to be patched.</td></tr> </table> <p data-bbox="695 423 1990 570"><a href="https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p> <p data-bbox="695 618 1990 805">“Cisco AMP for Endpoints Outbreak Control gives you a suite of capabilities to effectively <u>stop the spread of malware and malware-related activities</u>, like call-back communications or dropped file execution, without waiting for updates from your security vendor. This gives you the <u>power to move directly from investigation to control with a few mouse clicks, significantly reducing the time a threat has to spread or do more damage and the time it normally takes to put controls in place.</u>”</p> <p data-bbox="695 813 1990 959"><a href="https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p> <p data-bbox="695 1008 898 1036"><b>“Main Features</b></p> <p data-bbox="695 1044 1923 1114">AMP’s continuous analysis and retrospective security capabilities are made possible because of these robust features:</p> <p data-bbox="695 1130 730 1157">...</p> <ul data-bbox="695 1166 1990 1349" style="list-style-type: none"> <li>• <b>Static and dynamic malware analysis:</b> A highly secure sandboxing environment helps you <u>run, analyze, and test malware in order to discover previously unknown zero-day threats</u>. Integration of Threat Grid’s sandboxing and static and dynamic malware analysis technology into AMP solutions results in a more comprehensive analysis checked against a larger set of behavioral indicators.</li> </ul> <p data-bbox="695 1365 730 1393">...</p>		payload, and zero-day attacks on software vulnerabilities yet to be patched.
	payload, and zero-day attacks on software vulnerabilities yet to be patched.		

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability
	<ul style="list-style-type: none"> <li>• <b>Outbreak control:</b> <u>Achieve control over suspicious files or outbreaks and remediate an infection without waiting for a content update. Within the outbreak control feature:</u> <ul style="list-style-type: none"> <li>• Simple custom detections can <u>quickly block a specific file across all or selected systems</u></li> <li>• Advanced custom signatures can <u>block families of polymorphic malware</u></li> <li>• Application blocking lists can <u>enforce application policies or contain a compromised application</u> being used as a malware gateway and stop the reinfection cycle</li> <li>• Custom whitelists will help ensure that safe, custom, or mission-critical applications continue to run no matter what</li> <li>• Device flow correlation will <u>stop malware call-back communications at the source</u>, especially for remote endpoints outside the corporate network”</li> </ul> </li> </ul> <p><a href="https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p>
<p>wherein the computer program product is operable such that one or more of the plurality of mitigation techniques is identified based on an identification of an operating system.</p>	<p>Cisco Advanced Malware Protection (AMP) includes <i>wherein the computer program product is operable such that one or more of the plurality of mitigation techniques (e.g., the static and dynamic malware analysis and/or outbreak control, etc.) is identified based on an identification of an operating system (e.g., a Windows, Mac, Linux, and/or Android operating system, etc.).</i></p> <p><b>“Main Features</b></p> <p>AMP’s continuous analysis and retrospective security capabilities are made possible because of these robust features:</p> <p>...</p> <ul style="list-style-type: none"> <li>• <b>Static and dynamic malware analysis:</b> A highly secure sandboxing environment helps you <u>run, analyze, and test malware in order to discover previously unknown zero-day threats</u>. Integration of Threat Grid’s sandboxing and static and dynamic malware analysis technology into AMP solutions results in a more comprehensive analysis checked against a larger set of behavioral indicators.</li> </ul> <p>...</p>

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability				
	<ul style="list-style-type: none"> <li>• <b>Outbreak control:</b> <u>Achieve control over suspicious files or outbreaks and remediate an infection without waiting for a content update. Within the outbreak control feature:</u> <ul style="list-style-type: none"> <li>• Simple custom detections can <u>quickly block a specific file across all or selected systems</u></li> <li>• Advanced custom signatures can <u>block families of polymorphic malware</u></li> <li>• Application blocking lists can <u>enforce application policies or contain a compromised application</u> being used as a malware gateway and stop the reinfection cycle</li> <li>• Custom whitelists will help ensure that safe, custom, or mission-critical applications continue to run no matter what</li> <li>• Device flow correlation will <u>stop malware call-back communications at the source</u>, especially for remote endpoints outside the corporate network”</li> </ul> </li> </ul> <p>...</p> <p><b>Deployment Options for Protection Everywhere</b></p> <p>Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, the AMP solution can be deployed at different control points throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:”</p> <table border="1"> <thead> <tr> <th>Product Name</th><th>Details</th></tr> </thead> <tbody> <tr> <td>Cisco AMP for Endpoints</td><td><u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector</u>, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.</td></tr> </tbody> </table>	Product Name	Details	Cisco AMP for Endpoints	<u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector</u> , with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.
Product Name	Details				
Cisco AMP for Endpoints	<u>Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP’s lightweight connector</u> , with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.				

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability						
	<p data-bbox="695 305 1919 378"><a href="https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a> (emphasis added)</p> <p data-bbox="695 423 1024 451"><b>“Software requirements”</b></p> <table border="1" data-bbox="695 496 1505 1385"> <tr> <td data-bbox="695 496 1056 1198">Cisco AMP for Endpoints</td><td data-bbox="1056 496 1505 1198"> <ul style="list-style-type: none"> <li>● Microsoft Windows XP with Service Pack 3 or later</li> <li>● Microsoft Windows Vista with Service Pack 2 or later</li> <li>● Microsoft Windows 7</li> <li>● Microsoft Windows 8 and 8.1</li> <li>● Microsoft Windows 10</li> <li>● Microsoft Windows Server 2003</li> <li>● Microsoft Windows Server 2008</li> <li>● Microsoft Windows Server 2012</li> <li>● Mac OS X 10.7 and later</li> <li>● Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3</li> <li>● Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3</li> </ul> </td></tr> <tr> <td data-bbox="695 1198 1056 1312">Cisco AMP for Endpoints on Android mobile devices</td><td data-bbox="1056 1198 1505 1312">Android version 2.1 and later</td></tr> <tr> <td data-bbox="695 1312 1056 1385">Cisco AMP for Endpoints on Apple iOS</td><td data-bbox="1056 1312 1505 1385">MDM supervised iOS version 11</td></tr> </table>	Cisco AMP for Endpoints	<ul style="list-style-type: none"> <li>● Microsoft Windows XP with Service Pack 3 or later</li> <li>● Microsoft Windows Vista with Service Pack 2 or later</li> <li>● Microsoft Windows 7</li> <li>● Microsoft Windows 8 and 8.1</li> <li>● Microsoft Windows 10</li> <li>● Microsoft Windows Server 2003</li> <li>● Microsoft Windows Server 2008</li> <li>● Microsoft Windows Server 2012</li> <li>● Mac OS X 10.7 and later</li> <li>● Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3</li> <li>● Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3</li> </ul>	Cisco AMP for Endpoints on Android mobile devices	Android version 2.1 and later	Cisco AMP for Endpoints on Apple iOS	MDM supervised iOS version 11
Cisco AMP for Endpoints	<ul style="list-style-type: none"> <li>● Microsoft Windows XP with Service Pack 3 or later</li> <li>● Microsoft Windows Vista with Service Pack 2 or later</li> <li>● Microsoft Windows 7</li> <li>● Microsoft Windows 8 and 8.1</li> <li>● Microsoft Windows 10</li> <li>● Microsoft Windows Server 2003</li> <li>● Microsoft Windows Server 2008</li> <li>● Microsoft Windows Server 2012</li> <li>● Mac OS X 10.7 and later</li> <li>● Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3</li> <li>● Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3</li> </ul>						
Cisco AMP for Endpoints on Android mobile devices	Android version 2.1 and later						
Cisco AMP for Endpoints on Apple iOS	MDM supervised iOS version 11						

## PRELIMINARY CLAIM CHART

Patent No. 9,100,431, Claim 14: Cisco Advanced Malware Protection (AMP) for Endpoints

Claim 14 Elements	Applicability
	<a href="https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html">https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/datasheet-c78-733181.html?referring_site=RE&amp;pos=1&amp;page=https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html</a>